Cleve House School and Little Cleve Nursery's Data Protection Policy

Complies with the Data Protection Act 1998
(with intention to meet requirements of the Data Protection Bill and GDPR from May 2018)

Chief Privacy Officer (CPO) - E Corcoran

Reviewed September 2020
To be reviewed: Annually

Next review: October 2021

Data Protection Policy and General Data Protection Regulation Policy

Scope: This Policy applies to Cleve House School and Little Cleve Nursery

Cleve House School collects and uses personal information about staff, students, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website, www.ico.org.uk

At the current time due to the advice given by 'Farrer and Co. October 2017.' (Appendix F) we do not need to appoint a Data Protection Officer only a Chief Privacy Officer (CPO). Clare Fraser, the Deputy Head, is the School's Chief Privacy Officer (CPO) and can be contacted at school on 0117 9777218 or at Clevehouseschool@btconnect.com . Schools also have a duty to issue a Fair Processing Notice to all parents/guardians; this summarises the information held on pupils, how it is securely held, why it is held and the other parties to whom it may be passed on. See Appendix D.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines. Guidance is provided in the attached Appendices A-E.

What is Personal Information?

Personal information or data is defined as data, which relates to a living individual who can be identified from that data or other information held. This may include, but is not limited to:

- Names
- Email Addresses
- Postal Addresses
- Phone Numbers
- Financial information

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

General Statement

Cleve House School is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information may be shared, and why and with whom it may be shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so and as indicated in the school's entry in the ICO Data Protection Register
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Complaints

Complaints will be dealt with in accordance with the school's complaints procedure. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed annually. The policy review will be undertaken by the Headmaster and Chief Privacy Officer.

Contacts

If you have any enquires in relation to this policy, please contact the Headmaster, Mr Craig Wardle, who will also act as the contact point for any subject access requests.
Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745 3

Linked documents:
Safeguarding Policy
Confidentiality Policy

To be reviewed OCT 2020

Ratified by Craig Wardle, Proprietor

Appendices

Appendix A - Procedures for responding to subject access requests
Appendix B - Data Protection Codes of Practice for Staff
Appendix C - Implementation: The processing of written documentation
Appendix D – Fair Processing Notice
Appendix E – Access to Personal Data Request
Appendix F - Farrer and Co. letter

Appendix A

Procedures for responding to subject access requests made under the Data Protection Act 1998.

Preservation of records

- In accordance with the Data Protection Act attendance registers are preserved indefinitely
- Students' records, including medical records, are kept for a minimum of 10 years after they leave the school
- The results of public examinations are kept indefinitely
- Master copies of notes and documents relating to staff appointments are retained for an appropriate period of time (e.g. six months) for unsuccessful candidates. For successful candidates, these notes and documents are kept in an employee's personal file
- Staff service records are kept for a minimum of 10 years after the member of staff has left the school
- School reports to parents and school prospectuses are kept indefinitely
- Accident reports are retained indefinitely
- All matters relating to school finance are retained for 7 years; receipts are retained for 10 years.
- Alumnae records are held indefinitely

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (England) Regulations 2005.

The following procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a Subject Access Request (SAR)

1. Requests for information from staff, students and others must be made in writing; which includes email, and be addressed to the Headmaster. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship if a child is involved. Evidence of identity can be established by requesting production of:
    - passport
    - driving licence
    - utility bills with the current address
    - Birth / Marriage certificate
    - P45/P60
    - Credit Card or Mortgage statement
      This list is not exhaustive.

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. Where a request is made by an individual with parental responsibility, a child with competency to understand can refuse to consent to the request for their records. This is subject to the perceived level of maturity of the child. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the subject access request on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:
    - Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
    - Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
    - If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 30 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However, the 30 days will not commence until after receipt of fees or clarification of information sought.

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore, all information will be reviewed prior to disclosure.**

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 30 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information, then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Proprietor, Craig Wardle, who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints, which are not appropriate to be dealt with through the school's complaint procedure, can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Appendix B

Data Protection Codes of Practice for Staff

a) When writing minutes, memoranda, sending notes or letters, or sending e-mails the composer must think about the level of confidentiality involved and question whether the proposed method of communication is appropriate. The names of pupils, colleagues or parents are never used in the 'subject field' of an email; a generic title must be used instead e.g. Key Stage 1 student. When using computers care must be taken to ensure sensitive materials are not stored in the wrong folder.

b) Strictly confidential material should be placed in an envelope, marked "Strictly Confidential", and given to the Headmaster. This should remain sealed, except when in use. The Headmaster should decide when this material should be accessed and by whom.

c) Important interviews with pupils about discipline problems or other concerns must be recorded, dated and signed. If a very sensitive issue is involved the pupil must be warned beforehand that what they say will be treated in confidence, but that another adult (staff or outside agency) may have to be called in. Parents may also be requested to be present unless there is a child protection issue.

d) Important interviews with parents/guardians about discipline problems or other concerns must be recorded, dated and signed. If a very sensitive issue is involved the parent or guardian must be warned that what they say will be treated in confidence, but that another member of staff or an outside agency may have to be called in.

e) Staff who are not directly involved in a medium to strictly confidential matter will only be told about it on a need-to-know basis.

f) The Child Record and Admissions database can be accessed by school office staff only and are enabled to make changes to the database, as set out within their job descriptions. A relevant subset of the child's record data is made available to the class teacher. Emergency contact information is available to all staff and first aiders.

g) The Financial database is accessible to Accounts staff only

h) No member of staff should give out information concerning any other member of staff or their family, or any pupil and her family (including telephone numbers), without first requesting permission to do so. When emailing multiple staff and parents, staff should ensure that email addresses are typed into the 'bcc' (blind carbon copy) to keep email addresses private.

i) Information concerning staff appointments and applications is strictly confidential to the people to whom it is delegated.

j) No document which mentions a third party may be seen by the subject of the documentation. If a document refers to person x and also to person y, x cannot see the document unless person y's identity is removed. Other documents concerning staff or students may be seen by the person / people to whom it / they relate upon request, providing a check with the third party has been carried out by the Headteacher or delegated representative, or details of the identity removed.

k) Cleve House School will ensure any use of online learning tools and systems are in line with privacy and data protection policies as followed within school. Online teaching follows the same principles as set out in the staff Code of Conduct.

l) If a staff member, student or a household member of a student were to contract COVID-19 and needed to self-isolate, names will not be shared with the school community.

Processing of visual images

Visual images in the form of photos, videos or other means are very often taken, recorded, used and sometimes retained in relation to school activities whether academic or otherwise.

1. Taking Visual Images for Personal Use
   The taking of visual images during school activities is permitted but parents and other persons attending such activities should be informed that such images can only be used for personal purposes.

2. Official School Use
   Members of staff take photographs for school purposes only e.g. photographs of a school trip as a record, and should be mindful of the responsibility to use them appropriately. The need to think carefully about the photographs and images which they take and store will be highlighted to staff during staff training in Child Protection issues and during new staff induction. This is to ensure that staff do not make themselves vulnerable to accusations of inappropriate use. Similarly, this will ensure that staff do not expose children to the possibility of their images being used inappropriately.

   Images may be stored on a school computer in the Staff Drive (this drive is available only to staff) or into the Dropbox file. All staff and children are to be encouraged to delete images from the school network, school cameras and iPads, which are no longer, needed for school purposes.

   The school should seek consent if they wish to use an image of a child for any purpose other than routine administration. Such consent is given by parents/guardians when they formally accept a place for their child at the school (and renewed annually) and is set out in the Standard Terms and Conditions, as are all school policies on the processing of data relating to the children.

   When a photographer is engaged by the school, the school will ensure that the photographer understands data protection considerations. The relationship between the school and the photographer is regulated by a written contract or letter of agreement, which stipulates that the photographer can only use the visual images for the purposes as indicated by the school.

   Visual images of children form part of the historical records of the school and, as such, may be retained for an indefinite period of time.

Accessing school information remotely – Data Access

All staff are bound by the school's Acceptable Use of ICT policy guidance – See Safeguarding Policy

Data held on the school network cannot be accessed remotely. This data, including photographs of students, must not be stored on any personal device in accordance with the Safeguarding Policy. Remote access to the school email system is only available to the Proprietor, Headteacher and School Administrator via Gmail.

Personal use

Information made available through the remote access is confidential and protected by law under the Data Protection Act 1998.

- Users must not distribute or disclose any information obtained from remote school access to any person(s) with the exception of the student to which the information relates or to other adults with parental responsibility

- Users should not attempt to access the network in any environment where the security of the information may be placed at risk.

Appendix C

Implementation: The processing of written documentation

The following places may contain documentation concerning students, families and staff :

The Headmaster's Study	Private and Confidential Information, including report files,
School Office	Staff and Children's files, Personal data for students (past and present), parents (past and present), staff (past and present) information on new students, Safeguarding Files, staff information board and general information
Attic in 252B Room	Diaries, Registers, Pupils assessment files, Out of date office paperwork. Personal data for students (past and present)
SENCo room	SEND records, assessments and general information
Classrooms	Notes in children's books, planners, emails, registers and general information
Staff Room and School Office	Allergy Information
Form 4	Welfare, Some safeguarding, Data Protection and Bullying files

Digital information that can be accessed through the computer network.
The following table outlines user access rights to the school's network.

Drives Available	**Staff Access**	**Pupil Access**
Student Drive	Yes	Yes
Staff Drive	Restricted to selected users	No
Email	Yes	No

The information gathered and kept within the school may be divided into five types:

A. **Very low in confidentiality: access by any staff member; the child or their parent/guardian by arrangement**
   - Termly Progress Reports re Standard of Work and Attitude –
   - Copies of students' annual full reports and progress reports
   - Copies of personal assessment documentation e.g. targets
   - Marks/examination results (internal & external)

B. **Low in confidentiality: access by any member of staff; the child or their parent/guardian by arrangement.**
   - Baseline Test results
   - Information supplied by prior schools/nurseries

- Addresses and telephone numbers of separated parents/guardians
- Enquiries about entry to the school
- Information concerning individual pupils: Statements of Special Educational Needs, Learning Difficulties and Disabilities and English as a Foreign Language.
- Minutes of staff meetings

C. **Mid-range confidentiality: access by Headteacher, senior members of staff; the child or their parent/guardian by arrangement**.
   - Memoranda about any concerns (e.g. bullying)
   - Incident forms
   - Minutes of Senior Management Team meetings

D. **Strictly confidential: access by the Headteache and others by delegation**.
   - References written for children / other schools / children
   - Information about separated parents/guardians
   - Information about assisted places / bursaries
   - Sensitive information about which child, parent/guardian or staff ask for strictest confidentiality
   - Information concerning abuse – matters covered by the Children's Act
   - Staff records
   - Information about parents'/guardians' financial applications

E. Medical confidentiality: **access by the Headteacher, Secretary, SENCo and others by delegation on a 'need to know' basis only.**
   - Medical Records
   - Information re medical conditions

N.B. Health professionals are bound by the medical code of confidentiality in their work.

Outside Agencies

Where outside agencies and others provide support for the PSHE and citizenship provision, they must be made aware of, and abide by, the school's policies for PSHE, including disclosures and confidentiality. However, they may also have a role in providing advice and support directly to children. The boundary between these two roles must be agreed with the school. Children must be clear about what their rights to confidentiality are.

All teaching staff should be aware of the school's guidelines on letter writing on when and how communications should be sent to parents/guardians. In the cases of letters and replies, staff should examine the above list to ensure the correct degree of confidentiality.

Appendix D

Fair Processing Notice

Who processes your information?

Cleve House School is the data controller of the personal information you provide to us.
This means the school determines the purposes for which, and the manner in which, any personal data relating to pupils and their families is to be processed. Clare Fraser is the Chief Protection Officer. Her role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with the GDPR. She acts as a representative for the school with regard to its data controller responsibilities; she can be contacted on 0117 9777218 or at clevehouseschool@btconnect.com

In some cases, your data will be outsourced to a third party processor; however, this will only be done with your consent, unless the law requires the school to share your data. Where the school outsources data to a third party processor, the same data protection standards that Cleve House School upholds are imposed on the processor.

Why do we collect and use your information?

Cleve House School holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, Local Authority (LA) and/or the Department for Education (DfE).

We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013 In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

- To support pupil learning
- To monitor and report on pupil progress
- To provide appropriate pastoral care
- To assess the quality of our service
- To comply with the law regarding data sharing
- To safeguard pupils

Which data is collected?

The categories of pupil information that the school collects, holds and shares include the following:

- Personal information – e.g. names, pupil numbers and addresses
- Characteristics – e.g. ethnicity, language, nationality, country of birth
- Attendance information – e.g. number of absences and absence reasons
- Assessment information – e.g. national curriculum assessment results
- Relevant medical information
- Information relating to SEND
- Behavioural information – e.g. number of temporary exclusions

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, the school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

How long is your data stored for?

Personal data relating to pupils at Cleve House School and Little Cleve Nursery and their families is stored in line with the school's Data Protection Policy. See Appendix A

In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

Will my information be shared?

The school is required to share pupils' data with the DfE on a statutory basis.

Cleve House School and Little Cleve Nursery will not share your personal information with any third parties without your consent, unless the law allows us to do so.
The school routinely shares relevant pupils' and parents' information with:

- Pupils' destinations upon leaving the school
- The LA
- The NHS
- The DfE

What are your rights?

Parents and pupils have the following rights in relation to the processing of their personal data.
You have the right to:

- Be informed about how Cleve House School uses your personal data.
- Request access to the personal data that Cleve House School holds.
- Request that your personal data is amended if it is inaccurate or incomplete.
- Request that your personal data is erased where there is no compelling reason for its continued
- processing.
- Request that the processing of your data is restricted.
- Object to your personal data being processed.

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way Cleve House School and/or the DfE is collecting or using your personal data, you can raise a concern with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

Where can you find out more information?

If you would like to find out more information about how we and/or the DfE collect, use and store your personal data, please visit our website (www.clevehouseschool.) where you can download our Data Protection Policy.

Fair Processing Statement Cleve House School & Little Cleve Nursery

Cleve House School and Little Cleve Nursery, Bristol handles personal information in compliance with the Data Protection Act 1998 (the Act). We recognise the importance of the correct and lawful processing of personal data in maintaining confidence in our operations. We fully endorse and adhere to the principles set out in the Act.

CHS Ltd. and LCN Ltd. registration as a data controller

Cleve House School and Little Cleve Nursery is a 'data controller' under the Act. They hold information for the reasons given to the Information Commissioner and may use the information for any of those reasons.

Cleve House School and Little Cleve Nursery has notified the Information Commissioner that we will process personal data to enable us to provide our childcare and education services to our clients, to maintain our own accounts and records and to support and manage our staff. The Information Commissioner describes the processing in a register, which is available to the public for inspection at http://www.ico.org.uk. Cleve House School and Little Cleve Nursery entry on this register can be viewed here.

The key reason we process personal data is in relation to the provision of childcare and education services to our clients. In particular, this relates to the provision of those services to clients who have their children being cared for by us, who provide us with their personal data about their children.

Personal data

This statement applies to the handling of personal data. This is data relating to a living individual who can be identified from the data, or from that data and other information, which we hold or which is likely to come into our possession. It includes names and email addresses of parents and carers who use our childcare and education services, in relation to our work for our clients. It also includes any expression of opinion about an individual or any indication of our intention in respect of them.

Processing information fairly and lawfully

Cleve House School Ltd. and Little Cleve Nursery processes information only where:
a) the law allows us to, or
b) you have given your consent, or
c) we have received a court order

Ensuring your personal information is safe and accurate

Cleve house School and Little Cleve Nursery ensures that information held on our computer systems and in our paper filing systems is secure to guard against unauthorised or unlawful processing or accidental loss, destruction of, or damage to personal data. In order to carry out its functions Cleve House School and Little Cleve Nursery may receive information about you from others or give information to others, but we can only do this in accordance with the law. Any third parties from whom we receive personal data or to whom we pass personal data are also required to comply with the Data Protection Act.

Cleve House School and Little Cleve Nursery only collects and records personal information that is necessary to carry out its functions, nothing more. The information that we record is based on fact and, where opinion is recorded, it is relevant and backed up by evidence. To the extent it is reasonable and appropriate to do so, Cleve House School and Little Cleve Nursery checks that the personal information being recorded is accurate.

Data sharing

Cleve House School and Little Cleve Nursery will only share personal data with those organisations that it is legally able to, and where sharing personal data is necessary we will comply with the Data Protection Act.

Retaining information

We will only retain the information if a business need exists. It is not kept longer than is necessary for that purpose. To this end, Cleve House School and Little Cleve Nursery have in place and apply a formal retention policy for recorded information.

Marketing

Cleve House School and Little Cleve Nursery will only contact individuals who have consented by email for marketing purposes and only in relation to the schools products and/or services. If you no longer wish to receive information from Cleve House School regarding our products and/or services please unsubscribe by using the link within them or by contacting the school directly.

Links to other websites

Cleve House School and Little Cleve Nursery are not responsible for the content or reliability of linked websites. Linking should not be taken as an endorsement of any kind. We cannot guarantee that links will work all of the time and we have no control over the availability of the linked pages.

Your rights to access your personal information

Under the Act you have the right to ask to see the information which Cleve House School and Little Cleve Nursery holds about you and why. If you want to see the information we hold about you then you must ask for the information in writing and give your full name and address. You should send your request to:

The Chief Protection Officer
Cleve House School,
254, Wells Road,
Bristol, BS2 4PN
email: clevehouseschool@btconnect.com

As noted above, in most cases relating to the provision of actuarial services Cleve House School and Little Cleve Nursery anticipates that data protection responsibilities would be held by Cleve House School and and our clients. Where our possession of your personal data originated from such a client, we are likely to pass on any requests for access to personal data to that client, rather than respond to you directly. We will give assistance to our clients as appropriate where they need help to deal with your request.

Cleve House School will respond directly to requests for access to personal data, we aim to comply as quickly as possible. We will ensure that we deal with requests within 30 days of receipt unless there is a reason for delay that is justifiable under the Data Protection Act.

Complaints about how we process your personal information

In the first instance, an individual should contact Cleve House School Ltd. Complaints should be addressed to:

The Headmaster
Cleve House School
Cleve House School
254, Wells Road,
Bristol, BS2 4PN
email: clevehouseschool@btconnect.com

Appendix E

ACCESS TO PERSONAL DATA REQUEST

DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname……Enquirer's Forenames……..
Enquirer's Address ……
……
……
……
Enquirer's Postcode ……

Telephone Number …….

Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")? YES / NO

If NO,

Are you a parent as defined by the Education Act 1996 of a child who is the "Data Subject" of the records you are enquiring about? YES / NO

If YES,

Name of child or children about whose personal data records you are enquiring

_____

_____

Description of Concern / Area of Concern

_____

_____

_____

Description of Information or Topic(s) Requested (In your own words)

_____

_____

_____

Additional information.

_____

_____

_____

Please despatch Reply to: *(if different from enquirer's details as stated on this form)*

Name _____

Address _____

_____

_____

Postcode _____

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) ……

Name of "Data Subject" (or Subject's Parent) (PRINTED)…….

Dated ……

Appendix F

Data Protection Officers and independent schools: guidance on whether to appoint

One of the areas of the General Data Protection Regulation (GDPR) which has resulted in the most confusion in schools – and seen most mixed messaging from the many consultants and articles out there about GDPR – is the question of who will be caught by the new requirement for a mandatory Data Protection Officer (DPO), and what that title means.

The short answer – which may surprise some – is that independent schools will not, in most cases, need to appoint one. The question of whether they ought to do so voluntarily is more complex. However, for reasons discussed below, adopting what might be seen as the most cautious or compliant approach (i.e. appointing a DPO in time for 25 May 2018) is not necessarily the safest route, let alone the most practical and commercial.

Appointing a DPO unnecessarily could be an expensive misstep, but many schools are confused about the role and what it entails. The Information Commissioner (ICO) has yet to put out guidance, while the existing EU working party guidance clearly does not consider the legal position of the UK independent schools sector. For this reason ISBA considers there is a clear need for a detailed note on the topic aimed at independent schools.

1. What do we mean – and not mean – by a DPO?

This is an important issue to get straight at the outset. Under GDPR, a DPO may not be what you think it is. As a point of best practice – or, frequently enough, operational necessity – many schools already have a "Data Protection Officer", or someone of similar title, who more often than not is the bursar. In times past this simply meant the person in charge of most data decisions and administration at the school, most notably dealing with subject access requests and other potential distractions.

Some schools, in common with other organisations, erroneously refer to this person referred to as a "data controller" – a misunderstanding of a term that refers, in data protection law, to the school itself. Prior to 25 May 2018, by contrast, "Data Protection Officer" or "DPO" would be a very sensible job title to give that person, in line with both ICO terminology and market practice. However, as we shall see, calling anyone by that title after 25 May 2018 will carry a risk if the role is not intended to have the precise legal effect intended of it by GDPR.

The more formalised, carefully prescribed role of the DPO set out in the GDPR pushes an already unwelcome series of operational responsibilities and requirements to a higher level – and brings with it HR and accountability headaches. This is why schools should think carefully before appointing a DPO, or even re-appointing the same person to the role, after 25 May 2018.

2. Will your school legally require one?

The ICO acknowledges (as it did at the ISBA Cyber Security conference in October 2017) that for independent schools this position is by no means certain. Neither the GDPR wording nor the current EU working party guidance discloses a clear basis to suppose that most independent schools would be intended to be caught by the strict requirement.

This is contrast to the much clearer position with maintained schools, because all public authorities do indeed require a DPO. It may be that a single individual DPO will affix to the local authority as a whole rather than to each school, according them a degree of independence (as well as being cheaper of course, allowing oversight of numerous maintained schools): but this will depend on levels of access and capacity to deal with issues. As set out below, there may be lessons to learn for independent schools in observing what works best.

(i) The position with independent schools

For larger independent schools, it may be a relief that the draft GDPR requirement based on sheer numbers has not made it into the final regulation – for a time, it looked like any organisation of more than 250 people would require a DPO. Instead, the test is one of use and volume. Either

(a) do your “core activities” consist of either large-scale, systematic or regular monitoring of individuals?; or

(b) do your “core activities” relate to large-scale processing of special category personal data? (e.g. health, sexual life, ethnicity, religion – broadly the old “sensitive” categories).

The key terms here are “core activity” and “large scale”, and they are not further defined by GDPR. We are as yet lacking in clear and comprehensive guidance, but the EU working party guidance does draw some helpful conclusions. For example, it is the case that all employers are likely to process some special category data about their employees. However, while employing people is a necessary part of what they do, this does not make it their “core activity": it is ancillary to its main purpose.

A cautious analogy might be made to how schools process personal data of parents and, most obviously, pupils. Safeguarding, for example, is a core obligation on schools, and one which will properly involve both (a) the processing of sensitive personal data and (b) regular or systemic monitoring of staff and pupils. But the “core activity” of the school is education.

On balance, it might be safer to assume that a school's core activities *would* include processing special category data – but is it on a large scale? This is really where the DPO requirement looks less appropriate for most schools. "Large scale" is not defined but it would appear intended to cover bigger corporations who do market analysis, private health, tech companies and so on: it is unlikely to cover school communities of a few hundred people.

Considerations for what sort of larger independent school could be caught might, however, include:

- Do you hold a large amount of alumni data, and do you either monitor them or hold significant volumes of e.g. safeguarding files or incident reports?
- Do you have particularly intrusive monitoring systems?
- Is your school part of a large trust or multi-school business model where the "data controller" is likely to be the ultimate proprietor, i.e. the trustees or top company board?

If so, you might be looking at "large scale" processing activity of the sort that fits into either category, and consider the appointment of at least a single DPO for the entire group (where applicable). But until the ICO gives clear guidance on the topic, and lends some quantifiable measure to "large scale", there is something to be said for watching and waiting.

(ii) Comparison with other types of school

It will be of interest for the private schools sector to watch how the best practice position develops not simply with the ‘traditional’ state sector and academies, but also with more comparable models such as free schools and multi-academy trusts. These would qualify as public authorities, and require a DPO (albeit they are not always on all fours with maintained schools in how they are treated for certain other requirements of information law – e.g. a parent’s right to see the pupil file).

Structurally, and in terms of independence of decision making from local authorities (a key characteristic of a data controller being who actually determines what is done with personal data), such schools would seem to have more in common as data controllers with independents. Therefore independent schools should be vigilant as to developments elsewhere in education – even if they decide not to make the initial formal DPO appointment. It will be salutary to learn which DPO models work best in practice, especially for groups of schools, and which are less effective (or likely to have unintended consequences).

3. What are the expectations of the new DPO role?

Notwithstanding the lack of certainty in the law – or perhaps because of it – some schools are considering appointing a DPO voluntarily. Whether or not you are required to appoint a DPO by law, if you do appoint one then the following applies:

- **The DPO must possess "*expert knowledge of data protection law*".**

  This, notably, is not a requirement of IT expertise (although that might help!) but refers to a legal and practical understanding of how the law protects the privacy rights of individuals. GDPR values that over digital skills, and this seems particularly important in a schools context.

- **The DPO must be *properly*, and *promptly*, *involved* in all issues related to the protection of personal data at the school.**

  This runs from policy (at the outset) and overseeing privacy impact assessments, to dealing with requests from individuals (e.g. subject access) and whether and how to report data breaches to the ICO (which is mandatory within 72hrs if a certain threshold is reached) or affected individuals. Ultimately these decisions are for the school to make as data controller – hence the requirement for the DPO to be "*properly* [i.e. meaningfully] *involved*", i.e. to advise and inform, rather than having fully delegated responsibility.

- **The DPO can be an existing member of staff, or appointed to take on more than one role: being DPO does not have to be his/her sole responsibility...**

  This is consistent with the idea of course that a school can make an external appointment, or that one person can be DPO to several schools – provided there is sufficient access, in both directions, in each case (and sufficient independence from the interests of the governors / trustees / top company).

- **…however, a DPO must take sole responsibility for that role.**

  Responsibility is not the same as liability (rather the opposite – as explained below, the liability is ultimately with the school). What this means is that you cannot share the role across two or three staff members: the ICO expects a single person as their point of contact. This is in contrast to a more flexible team approach if your school does not make the formal appointment. Either way, depending on the size of your school, you may want data "champions" across several relevant departments (*administration / governance, IT, development, archives, legal/compliance, safeguarding, teaching staff etc.*) to assist the role.

- **The DPO must be independent, not too senior or conflicted…**

  EU working party guidance is clear that senior management, and specifically the heads of key departments like IT and HR, could be too conflicted to carry the role effectively and objectively. Similarly, bursars (and head teachers) are likely to be too aligned in their interests with the school to qualify: a DPO must speak truth to power, and make recommendations often against the organisation's short-term reputation or commercial interests.

- **…however, the DPO must have clout within the organisation.**

  They need to report to the highest level of management – the head, bursar and governors – and organisations are legally obliged to give them support, access, training and resources. As a compliance requirement, a DPO must be appointed "*on the basis of professional qualities*" and not simply appointed within the organisation based on who is willing to take on the role. Therefore schools might understandably wonder who at their organisation could possibly qualify, and indeed what they might expect to be paid on top of their existing salary.

- **The DPO's independence is protected at law.**

  Ultimately the DPO's duties are as much to the ICO and to the public (the school's "data subjects") as they are to the school. GDPR states that DPOs *"shall not be dismissed or penalised… for performing his* [or her] *tasks"* – something approaching "whistle-blower" type protections – and should not "*receive any instructions*" in how to carry out those tasks.

  In practice that definition of "instructions" may need to be explored: as above, it is ultimately for the data controller (school) to make decisions about whether to report a breach, disclose or amend a record, agree the terms of a contract with a data processor (e.g. cloud service provider), or go ahead

with a major IT revamp or fundraising campaign. But the practical consequences of leaning on a DPO not to disclose something under a subject access request or ignoring a recommendation (e.g. concerning breach reporting or the impact of a new measure) could be serious in enforcement terms.

- **The DPO has considerable record-keeping responsibilities.**

  This is not only a practical burden on the individual, but it is a core part of the accountability aspect of a school's GDPR compliance. Ultimately, if the school goes ahead with a major new project that might impact on individual privacy (e.g. marketing, CCTV, or monitoring), there should be a paper trail evidencing that this was thoroughly considered; and if a school has taken advice against a DPO's recommendation, the fact ought to have been recorded. The ongoing duty to assess and record the privacy impact of a decision continues even after the event.

- **When appointed, the DPO's details must be published and notified to the ICO.**

  The DPO's task includes a duty to "*cooperate with the supervisory authority*". One of the key tensions of the role is likely to be how the DPO balances duties to his or her paymaster with those to the regulator.

In summary, therefore, although designed to improve data protection practices at an organisation, the role of DPO brings with it considerable compliance and operative burdens in itself. For organisations like schools that are relatively small but extremely complex, and lacking substantial resources, it may be more attractive to adopt a more flexible approach than diving in to appoint a DPO.

4. If we decide not to appoint a DPO, what *do* we have to do?

As above, the ICO has not issued a clear position on DPOs and independent schools. Where the ICO is clear, in which regard ISBA and its lawyers are fully in agreement, is that any school will need to appoint a suitably trained, capable and competent person to take on the role of compliance lead at the organisation.

This person will require knowledge of data protection law, as well as being plugged in to the culture and structure of the school. In any event, the record keeping and accountability requirements of GDPR (as merely hinted at above) will need to be in place whether or not the person leading the charge is called a "DPO". So in fact, a school would want to go most of the way to appointing a role with all the qualities – and many of the responsibilities – of a DPO.

In doing so, the school would be well positioned to "flip" the role to a more formal appointment in the event that the ICO decided, down the line, that the Article 37 GDPR (the relevant section) had the effect of catching independent schools; or that such an appointment was always good practice in the sector; or if your school grew in size, or changed in structure, or started intensive monitoring. But there is a clear attraction in the meantime in waiting to see how the position pans out for others.

There is also a benefit in not having to appoint a new role; or allowing an outsider to have access to the school's most sensitive systems; or notably increase the burden and complexity of a valued existing employee's role. That is especially so, given the highly competitive employment market for individuals qualified to take on the DPO role (as either a full-time position or consultant) – and indeed the conflicting requirements about the person's required level of seniority, which does not lend itself well to an organisation the size of the average independent school.

5. If we are not appointing a DPO, what do we call them?

There is a final twist to this guidance. EU working party guidance is clear that to appoint anyone in a compliance lead role who is not intended to be a DPO, it must be clear to all (the public and the ICO) that this is indeed not intended. Calling them a DPO, or anything too close (School DPO, Officer for Data Protection, Data Processing Officer etc.) is therefore unwise and could well have the effect of requiring compliance to the high GDPR standard. Consider more imaginative (but descriptive) variations like Compliance Officer (Data), Privacy Officer, Head of Data Protection and so on.